暗号化ソフト VeraCrypt の使い方
(USB の暗号化も解説)

JCA-NET セミナー　2023/11/20

小倉利丸
toshi@jca.apc.org

大切なお知らせ

(1) セミナー新規申し込み
現状
セミナーの宣伝、告知をして、新規の参加申し込みがあった場合、本人の同意なしで、セミナーのメーリングリストの登録しています。

問題点
本来は、本人の希望をまず問い合わせた上で、メーリングリストへの登録を希望する人のみをメーリングリスト参加の手続きをとるべき。

解決策
本人の同意をとるようにします。

大切なお知らせ

(2) セミナー関連のメール、メーリングリストを二つに分けます。

- セミナーの告知やプレゼン資料などを配布するためのメールマガジンを設置 (seminar-info)
- セミナーでとりあげたテーマに関する質疑と、更に幅広くネットに関連する技術や政策あるいは市民運動などの情報の共有ができるメーリングリスト digital-rights を (現在の Linux-info とほぼ同じ役割になります)

※ Linux-info という名称を、実際のメーリングリストの内容にあわせて変更し、参加希望の有無をあらためてうかがいます。

大切なお知らせ

(3) 具体的に皆さんにやっていただきたいこと
皆さんの意向をうかがうことにします。
以下の選択肢から選んでいただくことになります。

- seminar-info のみに登録する
- semina-info と digital-rights の両方に登録する

上記の登録を下記のサイトでご自身で行なってください。
https://cryptpad.fr/form/#/2/form/view/jEsCvweOSFuKln9iNxIMCZHnW1pVUlf28RGPaDqm7jA/

暗号化ソフト VeraCrypt の使い方 (USB の暗号化も解説)

暗号化は、私たちの通信の秘密を確実なものにする最も不可欠な技術的手段です。
ネットにアクセスして様々な操作をするときには、私たちが特に自分で意識的に対処しなくても、様々な暗号化の仕組みが通信の舞台裏で作動していることが多くあります。
しかし、他方で、自分で自覚的に暗号化のための作業をしなければ暗号化されればい場合も多いのです。

- メールの暗号化
- ファイルの暗号化
- パソコンやハードディスク全体の暗号化

暗号化ソフト VeraCrypt の使い方（USB の暗号化も解説）

- メールの暗号化
  - 暗号化メールサービスを使う（Proton、 Tutanota など）
  - PGP などを用いで自分で暗号化する

メールの暗号化については今日のセミナーでは扱いません。今日は以下の二つに関連する暗号化の導入について紹介します。

- ファイルの暗号化
- パソコンやハードディスク全体の暗号化

暗号化ソフト VeraCrypt の使い方（USB の暗号化も解説）

暗号化とは、データを第三者には内容が判読できないようにすること。

実世界との類推でいうと金庫を設置して、そのなかに、大切なデータを保管することをイメージしてみてください。つまり、

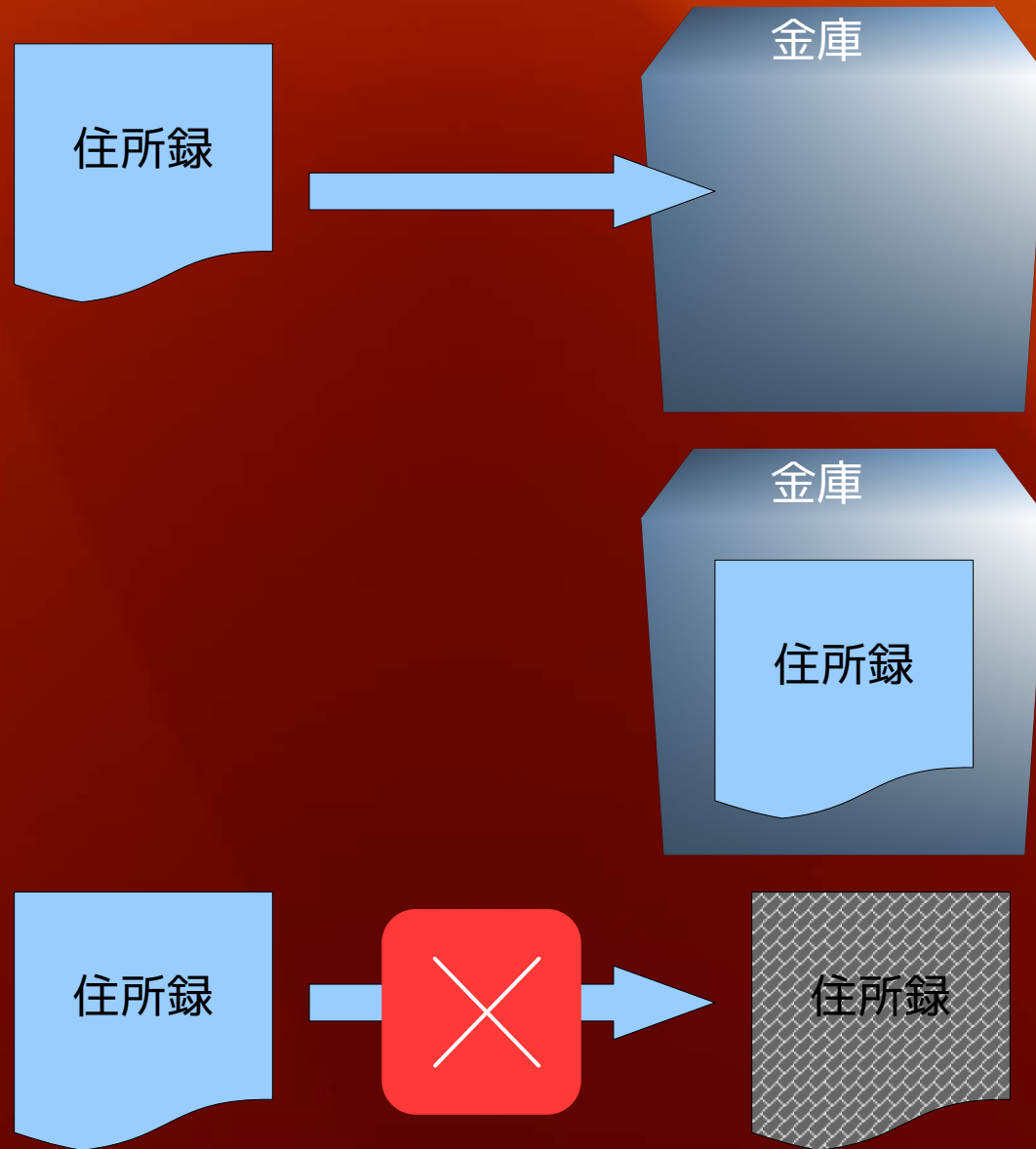
- 金庫を設置する
- 鍵をかけて閉める（あるいは鍵を開ける）

これと同じことを自分のパソコンで実現することになります。つまり ...

暗号化ソフト VeraCrypt の使い方 (USB の暗号化も解説)

•金庫を設置する
暗号化を実現するためのソフトウェアを自分のパソコンに設置する
•鍵をかけて閉める (あるいは鍵を開ける)
自分だけしか知らないパスワードで保護する

注意すること
•金庫の体積より大きなモノは保管できません。
•すでにあるデータを金庫のなかに入れて保護するのだから、データそのものを暗号化されたデータに変換するわけではなありません。

暗号化ソフト VeraCrypt の使い方（USB の暗号化も解説）

暗号化ソフト VeraCrypt の使い方 (USB の暗号化も解説)

手順

空の金庫を設置する (Veracrypt のソフトの導入)

設置した金庫にデータ (文書でも画像でも音楽でも何でも構わない) を入れる

金庫の鍵をかける

暗号化ソフト VeraCrypt の使い方（USB の暗号化も解説）

Veracrypt の導入方法

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/veracrypt-tutorial_1_jp/

VeraCrypt で USB を丸ごと暗号化

https://excesssecurity.com/veracrypt-usb-encryption/

暗号化ソフト VeraCrypt の使い方（USB の暗号化も解説）

Veracrypt は外付けのハードディスクや USB 全体を暗号化することができます。（私はバックアップ用の外付け HD を Veracrypt で暗号化している）

メリットでもありデメリットでもある？

- Veracrypt で暗号化された USB を他のパソコンに差しても読みこめません。
- ただし、他のパソコンに Veracrypt がインストールされている場合は、 USB にはアクセスできますが、パスワード（暗号化を行なった本人が設定したパスワードと、パソコンの持ち主のログインパスワードの両方が必要かもしれない）を入力しない限りデータにアクセスできません。

大切なお知らせ

(1) セミナー新規申し込み
現状
セミナーの宣伝、告知をして、新規の参加申し込みがあった場合、本人の同意なしで、セミナーのメーリングリストの登録しています。

問題点
本来は、本人の希望をまず問い合わせた上で、メーリングリストへの登録を希望する人のみをメーリングリスト参加の手続きをとるべき。

解決策
本人の同意をとるようにします。

大切なお知らせ

(2) セミナー関連のメール、メーリングリストを二つに分けます。

- セミナーの告知やプレゼン資料などを配布するためのメールマガジンを設置 (seminar-info)
- セミナーでとりあげたテーマに関する質疑と、更に幅広くネットに関連する技術や政策あるいは市民運動などの情報の共有ができるメーリングリスト digital-rights を (現在の Linux-info とほぼ同じ役割になります)

※ Linux-info という名称を、実際のメーリングリストの内容にあわせて変更し、参加希望の有無をあらためてうかがいます。

大切なお知らせ

(3) 具体的に皆さんにやっていただきたいこと
皆さんの意向をうかがうことにします。
以下の選択肢から選んでいただくことになります。

- seminar-info のみに登録する
- semina-info と digital-rights の両方に登録する

上記の登録を下記のサイトでご自身で行なってください。
https://cryptpad.fr/form/#/2/form/view/jEsCvweOSFuKln9iNxIMCZHnW1pVUlf28RGPaDqm7jA/